**REMARKS**

Claims 14, 15, and 25 have been amended to correct typographical errors noted by the Examiner. Claims 12-15, 18-27, 29-32, 42 and 43 are pending in this application.

Claims 12, 18-25, 29-32, 42 and 43 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leon (US 6,424,954) in view of Lertzman (US 2004/0006510). Claims 13-15, 26 and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leon and Lertzman in view of Mosher (US 5,799,322). Reconsideration is respectfully requested.

As noted in the current specification, in many instances it is desirable, or in some cases mandated by the postal authority, for value dispensing devices, e.g., postage meters, to maintain usage information. Such usage information can include, for example, the amount of postage dispensed by the meter, as well as other data, including, for example, total mail piece counts, piece counts for different classes of mail, piece counts for each different postage amount dispensed, etc. The usage information is typically compiled over a predetermined period of time, referred to as an audit period, such as, for example, weekly, monthly, or yearly. At the end of the determined audit period, the captured data for that audit period is transmitted to a data center, such as, for example, a data center operated by the meter manufacturer, where it is used to prepare reports. The prepared reports can be sent to the postal authority. These reports may then be utilized by the postal authorities (or the meter manufacturer) for such things, for example, as statistical analysis of use of the meter population, customer billing, etc.

There are problems, however, with conventional systems and methods for preparing data capture reports for a given audit period. One such problem is that the data capture data is blindly trusted for preparation of a report. The data capture data, however, may not be fully trustworthy when received from the postage meter. For example, since the usage information is not securely stored within the device, it is possible for a dishonest person to modify the data capture data before it is transmitted to the meter manufacturer. For example, the value of the total amount of postage dispensed during the audit period could be modified in such a way that this value is

made lower than the actual value used. In cases where the reports are used for billing purposes, the postal authority would under bill the customer, based on the modified data capture report, and thus the postal authority would be defrauded of funds due.

The present invention alleviates the problems associated with the prior art and provides a system and method that can detect tampering with data capture data, as well as verify the authenticity of data capture data, in a value dispensing system. At the beginning of an audit period, an audit record is generated by the postage meter that includes the current register values at the beginning of the audit period and a digital signature generated by the device. At the end of the audit period, a second audit record is generated by the postage meter that includes the register values at the end of the audit period and a digital signature generated by the device. This end of period audit record is then transmitted to the data center, along with the data capture data and the start of period audit record (if not previously transmitted to the data center). The data center, after obtaining both the end of period audit record and start of period audit record, will verify the digital signature of the both audit records. Successful verification of the digital signatures authenticates the device to the data center, and indicates that the register values are valid, as any modification of the data contained within the audit records would result in a failure of the signature verification. The data center can then reconcile the postage meter usage, i.e., register values, by comparing the difference between the register values from the start of period audit record and the end of period audit record with the values as contained within the data capture data for the audit period. Any discrepancies between these values indicate that the data capture data may not be correct, and a further investigation can be performed. If there are no discrepancies, the data capture data is deemed to be accurate and the data can be utilized to prepare reports with a high degree of certainty that it accurately reflects the actual usage of the postage meter. (See Specification, paragraphs [0022] through [0025]).

In view of the above, claim 12 is directed to a method for a data center to process usage data of a value dispensing device that comprises "receiving a first audit record from the value dispensing device, the first audit record generated by the value dispensing device at a start of an audit period, the first audit record including a value of

at least one register maintained by the value dispensing device at the start of the audit period and a first digital signature; receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature; receiving usage data from the value dispensing device for the audit period; determining that the first and second digital signatures verify; determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period; comparing the determined difference with corresponding data provided in the usage data; and if the determined difference correlates with the corresponding data provided in the usage data, generating a usage report for the value dispensing system based on the usage data."

Leon, in contrast is directed to a postage metering system in which an audit transaction is performed periodically to reset a timer. If the timer times out before an audit transaction is performed, the secure metering device (SMD) transitions to a state in which no further operation (except for an audit transaction) is permitted. A user requests an audit causing the host PC to send an audit request message to the SMD. The SMD then sends the host PC a signed message that includes the required information, which can include the current contents of the secure revenue registers, the device ID number, the current date and time, and a transaction serial number generated by the SMD. The host PC forwards the signed message to a system server, which receives and validates the message. As part of the processing, the system server authenticates the signed message using the SMD's public key and analyzes the data included in the message. The system server then sends the host PC a signed message that includes the response data, including the same device ID and transaction number from the message received earlier. The host PC forwards this signed message to the SMD, which validates the message by verifying the signature and determining if the message is of an expected type. If the signature is valid and the message is of an expected typed, the SMD determines if the data contents of the message is correct by verifying the transaction serial number. If the data is valid, the SMD resets the timer and transitions to an operating state. (Col. 18, line 30 to Col. 19, line15).

Thus, in Leon the system uses only a single audit record for the purpose of resetting a timer. There is no disclosure, teaching or suggestion in Leon of "receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature" as is recited in claim 12. In Leon, there is no second audit record generated at the end of an audit period. The system in Leon uses only a single audit record taken at a specific point in time. The Office Action appears to be contending that the audit requests in Leon sent at the end of one period are also considered to be sent at the beginning of a subsequent period, and therefore this single audit request in Leon is the same as a first audit record generated at the start of an audit period and a second audit record generated at the end of the audit period. It is unclear how a single audit request in Leon is analogous to a first audit report and a second audit report that are generated at different times. There is no disclosure, teaching or suggestion in Leon of "receiving a first audit record from the value dispensing device, the first audit record generated by the value dispensing device at a start of an audit period, the first audit record including a value of at least one register maintained by the value dispensing device at the start of the audit period and a first digital signature; receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature" as is recited in claim 12.

There is also no disclosure, teaching or suggestion in Leon of "receiving usage data from the value dispensing device for the audit period." While the messages in Leon may provide current information, there is nothing in Leon that describes any type of usage data for an audit period. The Office Action has not provided any indication as to where this feature is allegedly disclosed, taught or suggested in Leon.

There is also no disclosure, teaching or suggestion in Leon of generating a usage report for the value dispensing system based on the usage data if the determined difference correlates with the corresponding data provided in the usage data as is

recited in claim 12. The Office Action contends that Fig. 8F and Col. 62, lines 14-43, disclose this feature. As described in Col. 39 of Leon, Fig. 8F shows a diagram of a device status screen 890. The Status Screen 890 displays information about the SMD and the user, which may be helpful for tracking and troubleshooting by the provider or U.S. Postal Service. Fig. 8F of Leon is reproduced below.

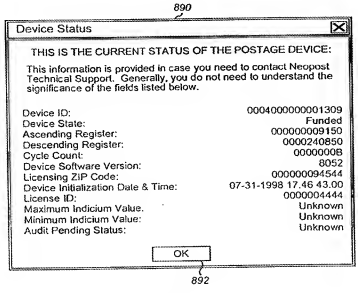



*FIG. 8F*

The current status of the postage device is not the same as a usage report generated based on usage data. With respect to Col. 62, as stated in Col. 62, lines 14-43, of Leon, if the Control Total is equal to the sum, the SMD increases the value of the internally stored Descending register, and prepares and sends a FUND4 message to the host PC. The SMD also records the Funding Revenue amount and the date and time of this Funding transaction, so it can report it as the previous values in the next Funding transaction. Increasing the value of the descending register is not the same as generating a usage report based on usage data. Furthermore, the FUND4 message is not a usage report – it merely is a status message to indicate the status of the postage download.

As noted in the Office Action, there is no disclosure, teaching or suggestion in Leon of "determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period" or "comparing the determined

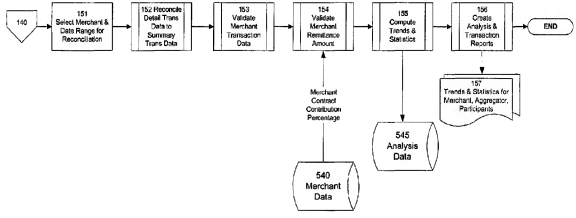
difference with corresponding data provided in the usage data" as is recited in claim 12. To overcome this deficiency, the Office Action relies on the reference to Lertzman. Lertzman is directed to a method and system for coordinating and managing rebates by a merchant of a portion of a purchase sale made by a participant to an aggregator. The aggregator, the participant, and the merchant register with one or more processor registries. A participant identification code is generated for the participant and a processor identification code is generated for the processor. When the participant initiates a purchase with the merchant, the participant identification code and amount of purchase transaction by the merchant are stored as sale tracking item. The stored participant identification code, the stored amount of purchase transaction, and funds corresponding to a portion of the amount of purchase transaction are sent to the processor. A portion of the funds received by the processor from the merchant are sent to the aggregator. (Paragraph [0013]).

Thus, as further described in Lertzman, when a purchase is made by a participant, the merchant stores the relevant participant's information, including a participant ID number. The purchase information of one or more participants is transmitted to the processor by the respective merchant. The processor then processes the data received from a plurality of merchants according to each aggregator, each participant, and each merchant. The processor then stores the processed data in a database. The stored data are made available to respective users with respective access rights. For example, a participant is given access only to information related to that participant. A merchant is not given any information with regard to the aggregator being supported by any particular participant. An aggregator is given access only to information related to that aggregator without disclosure of any private data (for example, where a participant shops and how much the participant spends) concerning any of the aggregator's participants. This scheme ensures the privacy of each user in addition to the security provided by the firewall. (Paragraph [0047]).

The Office Action contends that the periodic merchant report reconciliation process performed by the processor discloses the limitations of "determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period" and "comparing the determined difference with

corresponding data provided in the usage data" as is recited in claim 12. (Office Action, page 4). Applicants respectfully disagree.

As described in paragraphs [0074] and [0075] of Lertzman, a periodic merchant report is received by the processor. Subsequently the report is reviewed and verified against the funds received from merchant (142), and the format of the electronic report is verified or entered in the system (143). The merchant report file is imported (144) into database (500) and the database is updated. The processor database (500) tracks merchants, aggregator and participants, their interrelationships and transaction history for each entity. The process for the reconciliation of the Periodic Merchant Report (150) is illustrated in Fig. 10 of Lertzman, reproduced below.




The reconciliation process is initiated by selecting a merchant (40) and an applicable date range to be reconciled (151). Detail transaction data is reconciled to summary transaction data (152) by comparing the detail line items and amounts to the summary data by participant and merchant location. Transactions are then validated against merchant remittance amounts (153). Merchant summary, detail and financial information are also validated against the contract percentage from the database (500) among merchant data (540) (154). Statistical data relating to transactions and trends are stored in the database (500) among analysis data (545) (155). Analysis and transaction reports and statistics by merchant, aggregator and participant are computed (156) and reports created (157).

Thus, the system in Lertzman reconciles the detail transaction data to summary transaction data by comparing detail line items and amounts of the detail transaction data to the summary transaction data. This would entail reviewing each of the detailed transactions and ensuring that the amount for each detailed transaction corresponds to the amount reported in the summary. This is not the same as determining the difference between the value of a register included in audit records at the end of the audit period and the start of the audit period. There are no differences determined between two audit records in Lertzman. Furthermore, in Lertzman the amount that the merchant should have remitted is compared with the amount the merchant actually remitted to ensure the merchant remitted the proper amount. This is not the same as comparing a determined difference with corresponding data provided in usage data.

The Office Action contends that it would have been obvious to have modified the teachings of Leon to include the validation as taught by Lertzman in order to verify the remittance is proper for the transactions completed. Note, however, the Leon is not related in any way to verifying that remittance is proper for transactions completed. Further, combining the teachings of Leon to include validation to verify proper remittance does not arrive at the present invention. The combination of Leon with Lertzman will not cure any of the above deficiencies noted above – the combination still does not disclose, teach or suggest a method for a data center to process usage data of a value dispensing device that comprises "receiving a first audit record from the value dispensing device, the first audit record generated by the value dispensing device at a start of an audit period, the first audit record including a value of at least one register maintained by the value dispensing device at the start of the audit period and a first digital signature; receiving a second audit record from the value dispensing device, the second audit record generated by the value dispensing device at an end of the audit period, the second audit record including a value of the at least one register maintained by the value dispensing device at the end of the audit period and a second digital signature; receiving usage data from the value dispensing device for the audit period; determining that the first and second digital signatures verify; determining a difference between the value of the at least one register at the end of the audit period and the start of the audit period; comparing the determined difference with corresponding data provided in the usage data; and if the determined difference correlates with the

corresponding data provided in the usage data, generating a usage report for the value dispensing system based on the usage data" as is recited in claim 12.

For at least the above reasons, Applicants respectfully submit that claim 12 is allowable over the prior art of record. Claims 13-15, 18-24 and 42, dependent upon claim 12, are allowable along with claim 12 and on their own merits.

Claim 25 includes limitations similar to those of claim 12. For the same reasons given above with respect to claim 12, Applicants respectfully submit that claim 25 is allowable over the prior art of record. Claims 26, 27, 29-32 and 43, dependent upon claim 25, are allowable along with claim 25 and on their own merits.

In view of the foregoing amendments and remarks, it is respectfully submitted that all claims are in condition for allowance and favorable action thereon is requested.

Please charge any additional fees that may be required or credit any overpayment to Deposit Account Number 16-1885.

Respectfully submitted,

/Brian A. Lemm/
Brian A. Lemm
Reg. No. 43,748
Attorney for Applicants
Telephone (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
Shelton, CT 06484-8000